Abraham Schultz

1.a) Yes This check sum will detect errors caused by odd number of error bits.

- The XOR function is just a vertical parity check. If there is an odd number of errors, then there must be at least one column that contains an odd number of errors, and the parity bit will detect the error.

Additionally the RXOR function also catches all errors caused by an odd number of error bits. Each RXOR bit is a function of a unique spiral of bits in the block of data. if there is an odd number of errors, then there must also be be at least one spiral that contains the odd number of errors. And the error bit in that spiral will detect the error

1.b) NO, it is not possible to detect the errors.

- In order for both XOR an RXOR to fail, the pattern of error bits must have an intersection point between parity spirals and the parity columns such that there are even numbers of error bits in each spiral as well as in parity column.

1.c) This is probably to simple to be used as a secure Hash function.
It would be to easy to find multiple messages with the same Hash.

Yes

2.a) The given hash function fulfills the following hash function properties:

1. - hash function "H" can be applied to any size block of data

2. - hash function "H" produces a fixed-length of output

3. - Hash function "H(x)" is relatively easy to compute for any given x, and it makes both hardware and software implementations practical.

Abraham Sawitz HW #2

2.6)

$M = (189, 632, 900, 722, 349)$

$n = 989$

$h = \left(\sum_{i=1}^{5} (a_i)^2\right) \bmod n$

$h = (189^2 + 632^2 + 900^2 + 722^2 + 349^2) \bmod 989$

$= (35,721 + 399,424 + 810,000 + 521,284 + 121,801) \bmod 989$

$= 1,888,230 \bmod 989$

$= 229$

3.) $RSAH(B_1, B_2) = RSA(RSA(B1) \oplus (B2))$

if C1 and C2 are chosen arbitrarily

$\Rightarrow C2 = RSA(C1) \oplus RSA(B1) \oplus B2$

Encrypting first block and XOR the result

$RSA(C1) \oplus C2 = RSA(C1) + RSA(C1) + RSA(B1) \oplus B2$

$= RSA(B1) \oplus B2$

$\Rightarrow$ RSAH(C1, C2) is:

$RSAH(C1, C2) = RSA[RSA(C1) \oplus (C2)]$

The value of $RSA(C1) \oplus C2$ is equal to $RSA(B1) \oplus B2$

$\Rightarrow RSAH(C1, C2) = RSA[RSA(B1) \oplus B2]$

$\Rightarrow RSAH(C1, C2) = RSAH(B1, B2)$

Abraham Schultz HW # 2

4.a)

$p=3 \quad q=11 \quad e=7 \quad M=5$

$n = p \times q = 33$

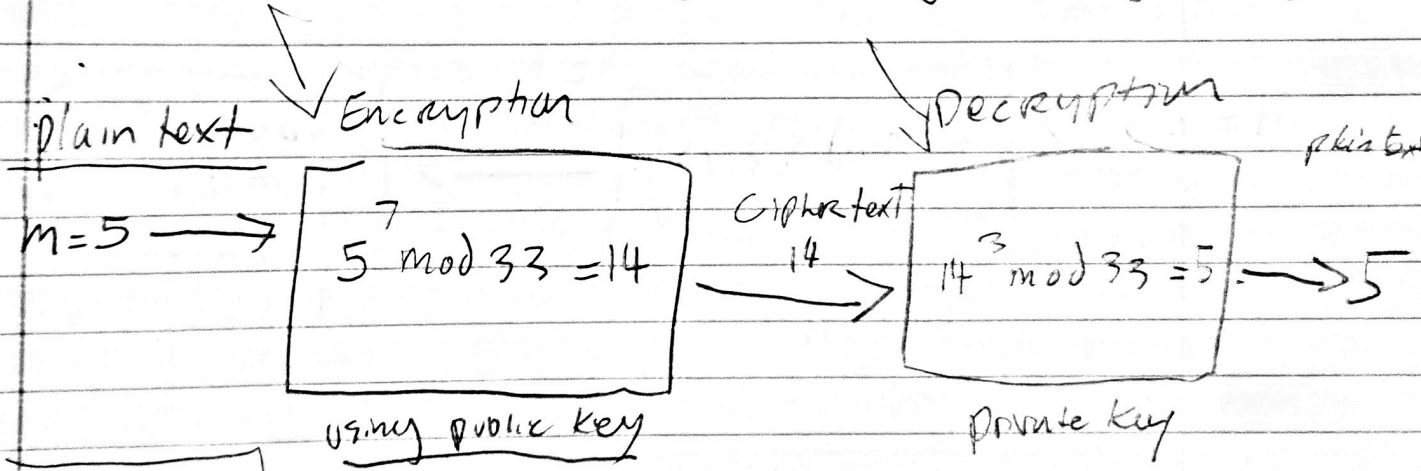
$\phi(n) = (p-1)(q-1) = (3-1)(11-1) = 2 \cdot 10 = 20$

$d < 20$

$de \bmod 20 = 1 \Rightarrow d(7) \bmod 20 = 1$

$3 \cdot 7 = 21 \quad 21 \bmod 20 = 1 \Rightarrow d = 3$

$KU = \{e, n\} = \{7, 33\} \quad KR = \{d, n\} = \{3, 33\}$



4.b)

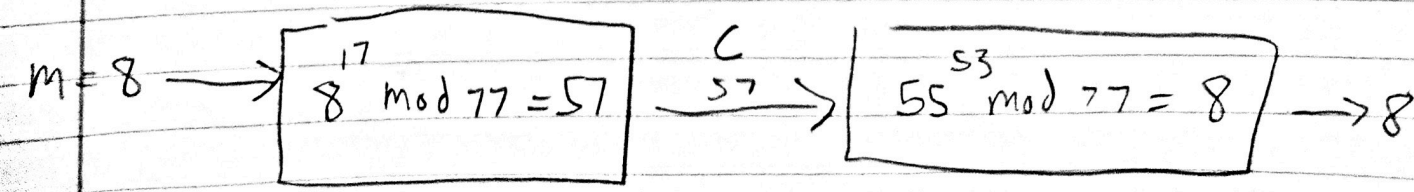
$p=7, \quad q=11, \quad e=17, \quad M=8$

$n = p \times q = 7 \cdot 11 = 77$

$\phi(n) = (p-1)(q-1) = (6-1)(11-1) = 60 \quad , \quad d < 60$

$d(17) \bmod 60 = 1 \qquad d = 53$

$KU = \{e, n\} = \{17, 77\} \quad KR = \{d, n\} = \{53, 77\}$



Abraham Schultz HW#2

4.c)

$p = 17,\ q = 31,\ e = 7,\ M = 2$

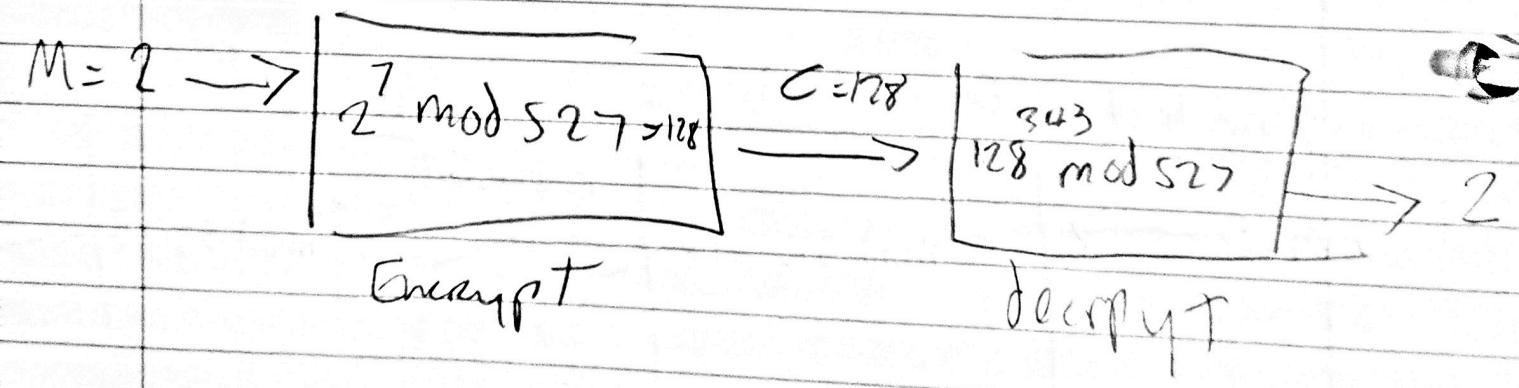
$n = p \times q = 17 \cdot 31 = 527$

$\phi(n) = (p-1)(q-1) = (17-1)(31-1) = 16 \cdot 30 = 480$

$d < 480$

$d = 343$ (I wrote python script for this)

$KU = \{e, n\} = \{7, 527\}$ $KR = \{d, n\} = \{343, 527\}$



Abraham Schultz HW#2.

5) This is insecure as even a large e as $M^e \bmod n$ amounts to $(e * (M \bmod n)) \bmod n$ and can be attacked by brute forcing values for M by calculating $M^e \bmod n$ for just the 26 values used and then comparing for plaintext that makes sense.

6.a) if user A has public key $Y_A = 9$, what is A's private key X_A

$Y_A = a^{x^A} \bmod q$; $9 = 2^{x^A} \bmod 11$; $2^6 = 64 \equiv 9 \bmod 11$; $X_A = 6$

6.b) if user B has public key $Y_B = 3$, what is the shared key K?

$K = (Y_B)^{X_A} \bmod q$; $K = (3)^6 \bmod 11$; $K = 3$